ONLINE CYBERSECURITY TRAINING

SPRING & SUMMER CATALOG 2019

"I love the material, I love the SANS Online delivery, and I want the entire industry to take these courses."

—Nick Sewell, IIT

Rewind | Revisit | Reinforce | Retain

Look Inside for NEW OnDemand Features, NEW Course Dates & NEW Courses

www.sans.org/online
Special Offers Available Now

Choose a tablet, laptop, or course discount offer with select OnDemand and vLive courses.

www.sans.org/online

Early bird discounts are available for Simulcast courses, see page 4 for more details.
“I love the flexibility that SANS Online Training offers, and being able to review and revisit content has helped me translate new skills into new work products.”
—William Amurgis, Baycare
Why Students Choose SANS OnDemand

- Four Months of Access to Comprehensive Online Training, Virtual Labs and Quizzes
- Access to GIAC-Certified Subject-Matter Experts
- Web-Based Training Accessible 24/7 from Your Desktop, Laptop, iPad, or Android Tablet
- No Travel or Time Away from the Office
- Includes Video, Labs, and Hands-On Exercises
- Complete Set of Books and Course Media
- Course Progress Reports
- Over 40 Courses Available – Anytime, Anywhere
- Perfect Preparation Tool for the GIAC Exam

The OnDemand platform couldn’t have been more convenient – having four months to complete my course allowed me to balance work, life, and training well.

-Jill Fraser, Jeffco

OnDemand

Train at your own pace anytime, anywhere with SANS OnDemand

More than 40 of SANS most popular information security courses are available via OnDemand, our proprietary online training platform. With four months of digital access to your course, quizzes, and labs, plus all of the corresponding printed books and materials, you’ll have plenty of time and resources to master your course content.

The benefits of taking your SANS training via OnDemand include:

• Live chat with GIAC-certified subject-matter experts gives you quick answers to questions and help with complex topics
• Rewind, fast forward, and pause options give you total control over the pace of your course
• Instruction directly from course authors means you will receive the best information security training available
• Progress tracking and quizzes keep you focused on achievement and content retention
• Search, bookmark, and note-taking options let you highlight sections you want to review or include in a study index
• Extended course access is perfect to prepare for GIAC Certification

If you lack a travel budget or simply appreciate having extended, fully supported access while training, OnDemand may be the best SANS training option for you.

New features in OnDemand:

- Closed Captioning
- Confidence Meter
- Social Media Links
- Video Pan/Zoom
- Adjustable Panel Sizing
- Course Progress Bar
- Dynamic Jump Back Button
- Take, Export, and Print Your Own Notes
- Adjustable Font Sizing
- Enhanced Keyboard Shortcuts and Accessibility Features

The OnDemand platform couldn’t have been more convenient – having four months to complete my course allowed me to balance work, life, and training well.

87,500

Students have completed high-quality SANS Online Training

2,200

InfoSec professionals access their SANS Online Training courses every week

Limited time SANS Online Training specials

Options include tablets, laptops, or discounts. For more information visit: www.sans.org/online

www.sans.org/ondemand
support@sans.org
301-654-SANS (7267)
## Courses

### Cyber Defense
- **SEC301: Introduction to Cyber Security** | GISP
- **SEC401: Security Essentials Bootcamp Style** | GSEC
- **SEC440: Critical Security Controls: Planning, Implementing, and Auditing**
- **SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis**
- **SEC501: Advanced Security Essentials – Enterprise Defender** | GCED
- **SEC503: Intrusion Detection In-Depth** | GCIA
- **SEC505: Securing Windows and PowerShell Automation** | GCWN
- **SEC506: Securing Linux/Unix** | GCUX
- **SEC511: Continuous Monitoring and Security Operations** | GMON
- **SEC524: Cloud Security and Risk Fundamentals**
- **SEC530: Defensible Security Architecture** | GDSA
- **SEC545: Cloud Security Architecture and Operations**
- **SEC555: SIEM with Tactical Analytics** | GCDA
- **SEC556: Implementing and Auditing the Critical Security Controls – In-Depth** | GCCC
- **SEC599: Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses** | GDAT

**Taught By**
- Keith Palmgren
- Dr. Eric Cole
- Randy Marchany
- Justin Henderson & John Hubbard
- Micah Hoffman
- Stephen Sims
- David Hoelzer
- Jason Fossen
- Hal Pomeranz
- Eric Conrad
- Dave Shackleford
- Eric Conrad
- Justin Henderson
- James Tarala
- Erik Van Buggenhout

### Penetration Testing
- **SEC460: Enterprise Threat and Vulnerability Assessment**
- **SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling** | GCIH
- **SEC542: Web App Penetration Testing and Ethical Hacking** | GWAPT
- **SEC600: Network Penetration Testing and Ethical Hacking** | GPN
- **SEC757: Mobile Device Security and Ethical Hacking** | GMOB
- **SEC617: Wireless Penetration Testing and Ethical Hacking** | GAWN
- **SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques**
- **SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking** | GXPN

**Taught By**
- Matt Toussain
- John Strand
- Eric Conrad
- Ed Skoudis
- Mark Baggett
- Joshua Wright
- Larry Pesce
- Adrien de Beaupre
- Stephen Sims

### Digital Forensics & Incident Response
- **FOR500: Windows Forensic Analysis** | GCFE
- **FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics** | GCFA
- **FOR518: Mac and iOS Forensic Analysis and Incident Response**
- **FOR526: Advanced Memory Forensics & Threat Detection**
- **FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response** | GNFA
- **FOR578: Cyber Threat Intelligence** | GCTI
- **FOR585: Smartphone Forensic Analysis In-Depth** | GASF
- **FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques** | GREM

**Taught By**
- Rob Lee
- Rob Lee
- Sarah Edwards
- Alissa Torres
- Philip Hagen
- Robert M. Lee
- Heather Mahalik
- Lenny Zeltser

### Security Management
- **MTG414: SANS Training Program for CISSP® Certification** | GISP
- **MTG433: SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program**
- **MTG512: Security Leadership Essentials for Managers** | GSLC
- **MTG514: IT Security Strategic Planning, Policy, and Leadership** | GSTRT

**Taught By**
- Eric Conrad
- Lance Spitzner
- Frank Kim
- Frank Kim

### Audit
- **AUD507: Auditing & Monitoring Networks, Perimeters, and Systems** | GSNA

**Taught By**
- David Hoelzer

### Legal
- **LEG523: Law of Data Security and Investigations** | GLEG

**Taught By**
- Benjamin Wright

### Development and Secure Coding
- **DEV522: Defending Web Applications Security Essentials** | GWEB
- **SEC534: Secure DevOps: A Practical Introduction**
- **SEC540: Cloud Security and DevOps Automation**
- **DEV541: Secure Coding in Java/JEE: Developing Defensible Applications**
- **DEV544: Secure Coding in .NET: Developing Defensible Applications**

**Taught By**
- Jason Lam
- Eric Johnson
- Gregory Leonard
- Eric Johnson

### Industrial Control Systems
- **ICS410: ICS/SCADA Security Essentials** | GICSP
- **ICS515: ICS Active Defense and Incident Response** | GRID

**Taught By**
- Justin Searle
- Robert M. Lee
Stream live SANS training to your home or office

Experience live SANS training without traveling by taking your information security course via Simulcast. You’ll experience the audio and video feeds streamed directly from the classroom to your laptop, plus real-time interaction with the moderator, peers, and teaching assistants. In addition, you will have access to lecture archives, the online lab environment, and live chat and email support from GIAC-certified subject-matter experts for four months. As a Simulcast student, you will receive the same courseware materials you would receive in a live course, shipped right to your home or office.

All Simulcast courses are recorded and archived, so if you miss part or all of any lessons, you will still have four months of access to the archived course content for review.

The benefits of taking your SANS training on the Simulcast platform include:

- Live, scheduled daytime sessions with SANS Certified Instructors
- In-class moderators who actively convey your questions to the instructor and ensure an interactive experience
- Teaching assistants available to support complex content and lab questions during your training sessions
- No travel, which extends training dollars and saves time
- The same instruction and learning outcomes as live training, with an additional four months of online access to absorb the course content

More courses are available, visit www.sans.org/simulcast for more information

<table>
<thead>
<tr>
<th>Course</th>
<th>Dates</th>
<th>Courses</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Security West (PST)</td>
<td>May 9-16, 2019</td>
<td>10</td>
</tr>
<tr>
<td>SANS San Antonio (CST)</td>
<td>May 28 – Jun 2, 2019</td>
<td>5</td>
</tr>
<tr>
<td>SANSFIRE (EST)</td>
<td>Jun 15-22, 2019</td>
<td>9</td>
</tr>
<tr>
<td>SANS Pittsburgh (EST)</td>
<td>Jul 8-13, 2019</td>
<td>4</td>
</tr>
<tr>
<td>SANS Rocky Mountain (MST)</td>
<td>Jul 15-20, 2019</td>
<td>4</td>
</tr>
<tr>
<td>DFIR Summit &amp; Training (CST)</td>
<td>Jul 27 – Aug 1, 2019</td>
<td>7</td>
</tr>
<tr>
<td>SANS Network Security (PST)</td>
<td>Sep 9-16, 2019</td>
<td>10</td>
</tr>
</tbody>
</table>

Limited time SANS Online Training specials

EarlyBird course discounts are available for SANS Simulcast courses. Check www.sans.org/simulcast for course and discount deadline information.

---

Why Students Choose SANS Simulcast

- Complete a Course in One Week
- Access Live training remotely via the virtual classroom
- Four Months of Online Course Access
- Labs, Hands-On Exercises, and Archived Lectures
- GIAC-Certified Subject-Matter-Expert Support
- Complete Set of Books and Course Media
- No Travel Required

---

“ I’m at home taking the Online Simulcast class but I feel like I’m there in the room. I don’t feel isolated at all. I just have access to my comforts while taking the class.”

- Deona Vastine, State of California

---

www.sans.org/simulcast
support@sans.org
301-654-SANS (7267)
vLive is an excellent way to get the best of both worlds – live, interactive SANS training from leading information security practitioners in the comfort of your own home or office. vLive sessions are scheduled in the evening to avoid conflict with your work schedule and feature smaller class sizes that give you an opportunity to connect directly with instructors and peers via the embedded Live Chat Feature. Simply log in at the scheduled times and join your instructor and classmates in an interactive virtual classroom. Don’t worry if you can’t attend every live session; classes are recorded and you can review the class archives for six months.

**Why Students Choose SANS vLive**

- Live Evening Courses Taken from the Convenience of Your Home or Office
- Direct Interaction with your Instructor and Peers via Interactive Chat Feature
- Pace of Training Cited as Key Benefit by vLive Student Alumni
- Six Months of Access to Labs, Hands-on Exercises, and Archived Lectures
- Access to Highly Qualified Subject-Matter Experts

“As always, vLive is the best balance between work, family, and continuing education.”
- Cameron Doherty, SCE

**Train live online in the evenings with the SANS Institute’s top instructors**

The benefits of taking your SANS training on the vLive platform include:

- Two conveniently scheduled 3-hour evening sessions (7-10pm EST) per week over six weeks
- The opportunity to preview content before a session or review content between sessions
- Lecture archives and lab environment available for six months, allowing you to revisit your training for improved retention
- Printed books and materials to facilitate GIAC Certification preparation and testing
- Downloadable MP3s for additional perspectives and experiences
- Access to subject-matter experts via Live Chat and email to get quick answers about complex content or lab questions

**More courses are available, visit www.sans.org/vlive for more information**

<table>
<thead>
<tr>
<th>Course</th>
<th>Dates</th>
<th>Instructors</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC503: Intrusion Detection In-Depth</td>
<td>Apr 24 – May 30, 2019</td>
<td>Ismael Valenzuela</td>
</tr>
<tr>
<td>SEC560: Network Penetration Testing and Ethical Hacking</td>
<td>Apr 30 – Jun 6, 2019</td>
<td>Moses Frost</td>
</tr>
<tr>
<td>MGT414: SANS Training Program for CISSP® Certification</td>
<td>May 6 – Jun 19, 2019</td>
<td>Ted Demopoulos, David R. Miller</td>
</tr>
<tr>
<td>SEC555: SIEM with Tactical Analytics</td>
<td>May 7 – Jun 13, 2019</td>
<td>John Hubbard</td>
</tr>
<tr>
<td>SEC566: Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td>May 21 – Jun 20, 2019</td>
<td>Chris Christianson, Brian Ventura</td>
</tr>
<tr>
<td>LEG523: Law of Data Security and Investigations</td>
<td>Jun 25 – Aug 1, 2019</td>
<td>Benjamin Wright</td>
</tr>
<tr>
<td>SEC599: Defeating Advanced Adversaries – Purple Team Tactics &amp; Kill Chain Defenses</td>
<td>Jul 8 – Aug 16, 2019</td>
<td>James Shewmaker, Alissa Torres</td>
</tr>
<tr>
<td>SEC511: Continuous Monitoring and Security Operations</td>
<td>Sep 3 – Oct 17, 2019</td>
<td>David Mashburn</td>
</tr>
</tbody>
</table>

New Dates

For more information visit: www.sans.org/online

Limited time SANS Online Training specials

Offers include tablets, laptops, or discounts.

For more information visit: www.sans.org/online

www.sans.org/vlive
support@sans.org
301-654-SANS (7267)
OnDemand Player

The SANS OnDemand player was custom built to give you control of your training experience. Below are just a few of the many popular features:

- Closed Captioning
- Confidence Meter
- Social Media Links
- Video Pan/Zoom
- Adjustable Panel Sizing
- Course Progress Bar
- Dynamic Jump Back Button
- Take, Export, and Print Your Own Notes
- Adjustable Font Sizing
- Enhanced Keyboard Shortcuts and Accessibility Features

Visit www.sans.org/demo to test drive your next SANS course today.
The SANS Voucher Program is a cybersecurity workforce training management system that allows you to easily procure and manage your organization’s training needs.

As a SANS Voucher Program participant, you will be able to:

- Provide your cybersecurity team with the highest standard of skill training and certification available
- Give employees a simple way to select and procure the training they need, when they need it
- Easily approve and manage student enrollment
- Monitor employee training progress and exam scores to ensure satisfactory completion
- Track investments, debits, and account balance for optimal budgeting

Voucher Funds purchased can be applied to any live and online SANS training courses, SANS Summit events, GIAC Certifications, or certification renewals.* Voucher Funds must be used within 12 months, but the term can be extended with additional investments.

Get Started
Visit www.sans.org/vouchers and submit the contact request form to have a SANS representative in your region call or email you within 24 business hours. Within as little time as one week, your eligible team members can begin their training.

*Current exceptions from the SANS Voucher Program are the Partnership program, Security Awareness training, and SANS workshops hosted at events run by other organizations.
About SANS

SANS Institute is the largest provider of information security training and education in the world.

Since 1989, SANS has trained more than 190,000 cybersecurity professionals—and delivered free news, research, and resources to many more. We’re the most trusted and, by far, the largest source of information security training and security certification in the world. We also develop, maintain, and provide free access to a vast collection of research documents about various aspects of information security.

100/100
Every company on the Fortune 100 list relies on SANS professional cybersecurity courses to train employees.

96%
of the professionals who’ve completed SANS training recommend it to their colleagues.

GIAC
30+ cybersecurity certifications are available in cyber defense, penetration testing, digital forensics, ICS/SCADA and more.
www.giac.org

NetWars
A suite of live and online hands-on interactive scenario challenges to help you master a wide range of skills.
www.sans.org/netwars

SANS Technology Institute
Accredited graduate programs and graduate certificates in information security completed via SANS training.
www.sans.edu

Internet Storm Center
Moment-by-moment intrusion detection news for the world’s cyber defense community.
isc.sans.edu

Securing The Human
Employee security awareness program applicable to every organization.
securingthehuman.sans.org

SANS CyberTalent
Provides innovative approaches to talent management for the InfoSec industry via training academies, talent assessments, and career fairs.
www.sans.org/cybertalent

Where to find SANS free resources:
Blogs: www.sans.org/security-resources/blogs
Webcasts: www.sans.org/webcasts
SANS Reading Room: www.sans.org/reading-room

Twitter: @SANSInstitute
LinkedIn: SANS Institute
Facebook: SANS Institute
More Training Formats

Private Training + Simulcast
for your dispersed workforce

SANS Private Online Training brings critical information security training directly to your workforce, regardless of their location. Our custom training programs incorporate both live and online instruction, and can be built for almost any SANS course. You’ll get a tailored experience built around your specific team’s size, location, and composition of learners. And by adding our Simulcast option, your organization can maximize its investment even further.

Private training environments allow students from commercial and government organizations to openly discuss sensitive issues and goals. All courses are led by SANS Certified Instructors; students can ask questions and interact with their instructor and peers during class and labs.

To explore your options for custom, distributed, live, and online workforce training from SANS, contact us at: privatetraining@sans.org | www.sans.org/private-training

SelfStudy
for the disciplined InfoSec student

The SANS SelfStudy program is self-paced training for the motivated and disciplined InfoSec student. It’s ideal for those who enjoy working independently, can’t travel for in-person training, or just prefer an extended study time via course books and MP3s.

Courses are now available in:

- Cyber Defense
- Penetration Testing
- Digital Forensics
- Incident Response
- Industrial Control Systems
- Developer
- Audit and Legal

To learn more or enroll, visit www.sans.org/selfstudy

NetWars
Test your cybersecurity know-how

A suite of live and online scenario challenges, SANS NetWars Experiences develop and test your cybersecurity know-how in a safe, interactive environment—all while having a little fun with your fellow IT security professionals.

In NetWars, students develop the real-world skills they’ll need to excel in their chosen fields. Participants learn on a cyber range while working through various challenge levels, all hands-on, while mastering the full range of proficiencies that information security professionals use in their jobs every day.
Extend and Validate Your Training

Combine the Flexibility of Online Training with the Power of GIAC Certification

Convenience and Flexibility

SANS Online Training offers several convenient training options to fit your learning style. Whether you are interested in anytime, anywhere access, live streaming from a SANS classroom, or live streaming during the evenings directly from your instructor, the flexibility of SANS Online Training will allow you to learn the skills necessary to prepare for GIAC Certification Exams.

With SANS OnDemand, SANS Simulcast, and SANS vLive, you’ll get:

- Content that helps you Rewind, Revisit, Reinforce, and Retain in order to help you study for your GIAC exam and retain your SANS knowledge long term.
- Four or More Months of Access
- Same Instructors as Live Events
- Same Content as Live Events
- Same GIAC Certification Test Results
- No Travel Required

Excellence and Capability

Broad, general InfoSec certifications are no longer enough: a SANS trained and GIAC certified workforce is necessary to combat today’s cyber threats. That’s because each GIAC certification focuses on specific job skills to ensure that professionals not only have the specialized knowledge to stay competitive in the marketplace, but also can defend and protect their organization/enterprise on day one.

Sign up for a GIAC Certification Attempt for only $769 when you add it during your Online Training course registration.

“Passed my @CertifyGIAC #GXPN this AM. What a great course! Glad I did the @SANSPenTest course #OnDemand. I rewatched the videos on advanced topics multiple times. Thanks, @Steph3nSims!”

-Mike Boya on Twitter

More Information

www.sans.org/online | www.giac.org
Broad, general InfoSec certifications are no longer enough: a SANS trained and GIAC certified workforce is necessary to combat today’s cyber threats. That’s because each GIAC certification focuses on specific job skills to ensure that professionals not only have the specialized knowledge to stay competitive in the marketplace, but also can defend and protect their organization/enterprise on day one.

Sign up for a GIAC Certification Attempt for only $769 when you add it during your Online Training course registration.

“Passed my @CertifyGIAC #GXPN this AM. What a great course! Glad I did the @SANSPenTest course #OnDemand. I rewatched the videos on advanced topics multiple times. Thanks, @Steph3nSims!”

- Mike Boya on Twitter

More Information
www.sans.org/online | www.giac.org

Combine the Flexibility of Online Training with the Power of GIAC Certification

SANS Online Training offers several convenient training options to fit your learning style. Whether you are interested in anytime, anywhere access, live streaming from a SANS classroom, or live streaming during the evenings directly from your instructor, the flexibility of SANS Online Training will allow you to learn the skills necessary to prepare for GIAC Certification Exams.

With SANS OnDemand, SANS Simulcast, and SANS vLive, you’ll get:

- Content that helps you Rewind, Revisit, Reinforce, and Retain in order to help you study for your GIAC exam and retain your SANS knowledge long term.
- Four or More Months of Access
- Same Instructors as Live Events
- Same Content as Live Events
- Same GIAC Certification Test Results
- No Travel Required

Experience NetWars Continuous

Play solo or on a team of up to five players

“NetWars takes the concepts in the class and gives you an opportunity to put them into action. Highly recommended!”

- Kyle McDaniel, Lenovo

So much more than a Capture-the-Flag event, NetWars Continuous is the online training program that guides you through hands-on lessons to locate vulnerabilities, exploit diverse machines, analyze systems, and defend your turf.

Fully executed online, NetWars Continuous includes automated hints and support from the SANS NetWars team to ensure that you have the most rewarding experience possible. The challenge also delivers 12 CPE credits upon completion.

Most importantly, you will walk away with confidence in your abilities and a scorecard that illustrates the areas in which you have demonstrated deep skills and security knowledge.

www.sans.org/netwars/continuous
Cyber Defense Essentials

All professionals entrusted with hands-on cybersecurity work should be trained to possess a common set of capabilities enabling them to secure systems, practice defense-in-depth, understand how attackers work, and manage incidents as they occur. To be secure, you should set a high bar for the baseline set of skills in your security organization.

SANS Cyber Defense Essentials courses help you build a solid foundation of core policies and practices to enable you and your security teams to practice proper incident response, then expand upon those crucial skills by adding advanced core techniques to help defend an enterprise from every angle.

Whether you’re new to security or need a broad overview of security topics, these courses will support your effort to win the battle against the wide range of cyber adversaries that want to harm environments.

“OnDemand really worked for me. It allowed me to take my time to read the material, stop and find supplemental information if needed, and stop the lecture and repeat sections.”

- Patricia Cohen, Institute for Defense Analyses
## Cyber Defense Essentials | Course List

### SEC301: Introduction to Cyber Security
This introductory course is the fastest way to get up to speed in information security. The entry-level course includes a broad spectrum of security topics and real-life examples and can be used to prepare for GISF Certification. [www.sans.org/SEC301](http://www.sans.org/SEC301)

### SEC401: Security Essentials Bootcamp Style
In this course, students learn the language and underlying theory of computer and information security. Since all jobs today require an understanding of security, this course will help you understand how security applies to your job. In addition, students will gain the essential and latest knowledge and skills required for effective management of security systems and processes. [www.sans.org/SEC401](http://www.sans.org/SEC401)

### SEC440: Critical Security Controls: Planning, Implementing, and Auditing
This 2-day course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS). These Critical Security Controls are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all serious and sensitive organizations. [www.sans.org/SEC440](http://www.sans.org/SEC440)

### SEC501: Advanced Security Essentials – Enterprise Defender
A key theme of this course is that prevention is ideal, but detection is a must. Security professionals must know how to constantly advance security efforts in order to prevent as many attacks as possible. This prevention needs to occur both externally and internally via portable, network and server environments. [www.sans.org/SEC501](http://www.sans.org/SEC501)

### SEC566: Implementing and Auditing the Critical Security Controls – In-Depth
As threats evolve, an organization’s security should evolve as well. To enable your organization to stay on top of this ever-changing scenario, SANS designed this course to train students how to implement the Twenty Critical Security Controls – a prioritized, risk-based approach to security that was designed by a master group of private and public sector experts from around the world. [www.sans.org/SEC566](http://www.sans.org/SEC566)

### SEC599: Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses
This course provides an in-depth understanding of how current adversaries operate and arms you with the knowledge and expertise you need to detect and respond to today’s threats. SEC599 aims to leverage the purple team concept by bringing together red and blue teams for maximum effect. The course focuses on current attack strategies and how they can be effectively mitigated and detected using a Kill Chain structure. [www.sans.org/SEC599](http://www.sans.org/SEC599)

## SEC599 & Purple Team

Although they share a common goal, Blue (defensive) and Red (offensive) Teams are not always well-aligned, which leads to most organizations not leveraging the full value of their teams’ overall expertise. The respective teams typically report to a different hierarchy, which leads to different objectives:

### Blue Team – Defense
1. Implementing Controls
2. Security Monitoring
3. Incident Response

### Red Team – Offense
1. Vulnerability Assessments
2. Penetration Tests
3. Social Engineering

The Purple Team concept brings Red and Blue together, encouraging the two teams to share insight and feedback to achieve one common goal.

**The Purple Team Common Goal = To improve organization security posture.**

Through real-world examples and lab exercises, SEC599 illustrates what adversaries are actually doing now, and how we can effectively combat their tactics using a Kill Chain structure.
Blue Team Operations

SANS Blue Team Operations courses teach you the critical skills required to defend your organization against cyber-attacks and improve its overall security posture.

**Blue Team = Defense**

The term Blue Team comes from the world of military simulation exercises. During exercises, the Red Team plays the role of the adversary (Offense), and the Blue Team acts as the friendly forces being attacked (Defense). Specifically emphasizing cybersecurity, the Blue Team’s focus is to defend the organization from digital/cyber attacks. To be Blue Team means developing and implementing multiple security controls in a layered defense-in-depth strategy, verifying their effectiveness, and continuously monitoring and improving defenses.

In theory, everything that improves defensive security posture could be classified as Blue Team, but true Blue Team Operations implies that there is an overt emphasis on discovering and defending against attacks. Security professionals must have intimate knowledge of their existing environments to assess their current states and attacks against them.

SANS Blue Team Operations courses give you the knowledge, tools, and techniques needed to defend your networks with insight and awareness, and will help you implement a modern security design that allows you to defend networks and understand threats. Monitoring and Detection education includes learning to build the network and endpoint security, then carefully navigate through automation and Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM).

**Seth Misenar**
Blue Team Operations
Co-Curriculum Lead
SANS Fellow

**Eric Conrad**
Blue Team Operations
Co-Curriculum Lead
SANS Fellow
Blue Team Operations | Course List

SEC455: SIEM Design & Implementation
This course will teach you how to build a Security Information and Event Management (SIEM) system from the ground up using the Elastic Stack. Students will learn the required stages of log collection, endpoint agent selection, logging formats, parsing, enrichment, storage, alerting, and how to combine these components to make a flexible, high-performance SIEM solution. www.sans.org/SEC455

SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis
This course is an entry-level introduction to open-source intelligence that teaches current, real-world skills, techniques, and tools that law enforcement, private investigators, cyber attackers, and defenders use to scour the massive amount of information across the Internet, analyze the results, and pivot on interesting pieces of data to find other areas for investigation. www.sans.org/SEC487

SEC503: Intrusion Detection In-Depth
This course teaches core knowledge, tools, and techniques that will help students who monitor and defend networks. Students will learn the theory of TCP/IP and popular application protocols like DNS and HTTP, to intelligently examine network traffic for signs of intrusions. Hands-on practice includes open-source tools like tcpdump, Wireshark, Snort, Bro, tshark, and SiLK. www.sans.org/SEC503

SEC505: Securing Windows and PowerShell Automation
In SEC505 students learn to defend against pass-the-hash attacks, administrator account compromise, and the lateral movement of hackers inside the network by implementing the Critical Security Controls and PowerShell in a Windows environment. www.sans.org/SEC505

SEC506: Securing Linux/Unix
SEC506 provides in-depth coverage of Linux and Unix security issues and examines how to mitigate or eliminate general problems that apply to all Unix-like operating systems. Specific configuration guidance and practical, real-world examples, tips, and tricks are provided to help students remove vulnerabilities. www.sans.org/SEC506

SEC511: Continuous Monitoring and Security Operations
The Defensible Security Architecture and Network Security Monitoring/Continuous Diagnostics and Mitigation/Continuous Security Monitoring taught in this course will best position your organization or Security Operations Center to analyze threats and detect anomalies that could indicate cybercriminal behavior. www.sans.org/SEC511

SEC524: Cloud Security and Risk Fundamentals
This two-day course teaches you how to properly evaluate cloud providers and perform risk assessment and review, with a focus on risk assessment versus technical implementation and operations. www.sans.org/SEC524

SEC530: Defensible Security Architecture and Engineering
Establish and maintain a holistic and layered approach to security balancing detection, prevention, and response capabilities, with implementation of appropriate controls on the network. Learn the fundamentals of defensible security architecture and how to engineer it. With a heavy focus on leveraging current infrastructure (and investment) students will learn how to reconfigure devices to significantly improve their organizations’ prevention capabilities in the face of today’s dynamic threat landscape. You will come away with recommendations and suggestions that will aid in building a robust security infrastructure. www.sans.org/SEC530

SEC545: Cloud Security Architecture and Operations
This course takes you from A to Z in the cloud, with everything ranging from policy, contracts, and governance to controls at all layers. Cloud architectures, IAM and encryption, and how offense and defense differ in the cloud. The course covers automation tactics that will help you work effectively with the DevOps teams, and build a sustainable cloud security program in your environment. www.sans.org/SEC545

SEC555: SIEM with Tactical Analytics
This course is designed to guide the student through the steps of tailoring and deploying Security Information Event Management (SIEM) to full Security Operations Center (SOC) integration. The underlying theme is to actively apply continuous monitoring and analysis techniques by utilizing modern cyber threat attacks. Labs involve replaying captured attack data to provide real-world results and visualizations. www.sans.org/SEC555
Penetration Testing

What makes SANS Penetration Testing courses special?

In SANS Penetration Testing courses, you will learn in-depth, hands-on skills associated with the most powerful and common attacks today.

- Penetration testers, vulnerability assessment personnel, and Red Teamers: You’ll be able to apply your skills in your very next engagement, providing even more technical depth and business value.
- Cyber defenders and Blue Teamers: You’ll gain key insights into offensive tactics that will help you significantly improve your organization’s defenses.
- Forensic analysts and incident handlers: You’ll transform your understanding of the adversary’s methods and be better able to anticipate and counter the attacker’s next move.

What is high-value penetration testing and why is it important? A high-value penetration test:

- Emulates the activities of real-world attackers
- Discovers vulnerabilities in target systems
- Exploits those vulnerabilities under controlled circumstances
- Applies technical excellence to determine and document risk and potential business impact
- Conducts professional and safe testing according to a carefully designed scope and rules of engagement
- Helps an organization with its goal of properly prioritizing resources
- Teaches skills that will help all cybersecurity professionals in their work of securing their organization.

“I’ve used several different platforms in the past and NONE have been so well put together as SANS OnDemand. I could go on and on about what I like about the interface and how well the material goes with the book and the labs go with both. Programmers, well done!”

- Francis Colvais, PYA
Penetration Testing | Course List

**SEC460: Enterprise Threat and Vulnerability Assessment**
Build technical vulnerability assessment skills and techniques, while highlighting time-tested practical approaches to ensure true value across the enterprise. The course covers threat management, introduces the core components of comprehensive vulnerability assessment, and provides the hands-on instruction necessary to produce a vigorous defensive strategy from day one. The course is focused on equipping information security personnel from mid-sized to large organizations charged with effectively and efficiently securing 10,000 or more systems. www.sans.org/SEC460

**SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling**
SEC504 will prepare you to turn the tables on computer attackers. This course addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still so prevalent, and everything in between. You will learn a time-tested, step-by-step process to respond to computer incidents; how attackers undermine systems so you can prepare, detect, and respond to them; and how to discover holes in your system before the bad guys do. www.sans.org/SEC504

**SEC542: Web App Penetration Testing and Ethical Hacking**
In SEC542, you will practice the art of exploiting web applications to find flaws in your enterprise’s web apps. Through detailed, hands-on exercises you will learn the four-step process for web application penetration testing; inject SQL into back-end databases to learn how attackers exfiltrate sensitive data; and utilize cross-site scripting attacks to dominate a target infrastructure. www.sans.org/SEC542

**SEC560: Network Penetration Testing and Ethical Hacking**
SEC560 prepares you to conduct successful penetration testing and ethical hacking projects. The course will teach you how to perform detailed reconnaissance, exploit target systems to gain access and measure real business risk, and scan target networks using best-of-breed tools in hands-on labs and exercises. www.sans.org/SEC560

**SEC573: Automating Information Security with Python**
SEC573 will prepare you to apply Python coding skills to do your job more effectively and efficiently. You will learn to tweak, customize, and develop your own tools to become a great penetration tester; develop applications that interact with networks, websites, databases, and file systems; and build practical applications that you can immediately put into use in your penetration tests. www.sans.org/SEC573

**SEC575: Mobile Device Security and Ethical Hacking**
SEC575 will prepare you to evaluate the security of mobile devices, effectively assess and identify flaws in mobile applications, and conduct a mobile device penetration test – all critical skills required to protect and defend mobile device deployments. www.sans.org/SEC575

**SEC617: Wireless Penetration Testing and Ethical Hacking**
SEC617 is designed for professionals seeking a comprehensive technical ability to understand, analyze, and defend the various wireless technologies that have become ubiquitous in our environments and, increasingly, key entrance points for attackers. You’ll receive the SANS Wireless Assessment Toolkit (SWAT), a collection of hardware and software tools to jumpstart your ability to assess wireless systems. www.sans.org/SEC617

**SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques**
SEC642 will teach you the advanced skills and techniques required to test modern web applications and next-generation technologies. In this course, you will learn through a combination of lectures, real-world experiences, and hands-on exercises that will teach you the techniques to test the security of tried-and-true internal enterprise web technologies, as well as cutting-edge Internet-facing applications. The course concludes with an intensive hands-on Capture-the-Flag challenge where you will apply the knowledge you have acquired throughout the course in a fun environment, based on real-world technologies. www.sans.org/SEC642

**SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking**
SEC660 is designed as a logical progression point for students who have completed SEC560, or for those with existing penetration testing experience. The course goes far beyond simple scanning for low-hanging fruit and teaches you how to model the abilities of an advanced attacker to find significant flaws in a target environment and demonstrate the business risk associated with these flaws. www.sans.org/SEC660
Digital Forensics and Incident Response

With today’s ever-changing technologies and environments, it is inevitable that every organization will deal with cybercrime. Adversaries are no longer compromising one or two systems in enterprises; they are compromising hundreds. Organizations of all sizes need personnel who can master incident response techniques to properly identify compromised systems, provide effective containment of the breach, and rapidly remediate the incident. Likewise, government and law enforcement agencies require skilled personnel to perform media exploitation and recover key evidence available on adversary systems and devices.

SANS DFIR courses will teach you to:

- Hunt for the adversary before and during an incident across your enterprise
- Acquire in-depth digital forensics knowledge of the Microsoft Windows and Apple OSX operating systems
- Examine portable smartphone and mobile devices to look for malware and digital forensic artifacts
- Incorporate network forensics into your investigations, providing better findings, and getting the job done faster
- Leave no stone unturned by incorporating memory forensics into your investigations
- Understand the capabilities of malware to derive threat intelligence, respond to information security incidents, and fortify defenses
- Identify, extract, prioritize, and leverage cyber threat intelligence from advanced persistent threat (APT) intrusions
- Recognize that a properly trained incident responder could be the only defense an organization has during a compromise

“SANS has created such an outstanding learning environment. Whether through its Online or In-Person training, the instructors and the content are far superior to anything else I have experienced. Keep up the great work.”

- Adam Fowler, GMAC
<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOR500</td>
<td>Windows Forensic Analysis</td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Incident Response, Threat Hunting, and Digital Forensics</td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Memory Forensics &amp; Threat Detection</td>
</tr>
<tr>
<td>FOR518</td>
<td>Mac and iOS Forensic Analysis and Incident Response</td>
</tr>
<tr>
<td>FOR526</td>
<td>Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response</td>
</tr>
<tr>
<td>FOR572</td>
<td>Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response</td>
</tr>
<tr>
<td>FOR578</td>
<td>Cyber Threat Intelligence</td>
</tr>
<tr>
<td>FOR585</td>
<td>Smartphone Forensic Analysis In-Depth</td>
</tr>
<tr>
<td>FOR610</td>
<td>Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td>
</tr>
</tbody>
</table>
# Course List

## Management Curriculum

**MGT414: SANS Training Program for CISSP® Certification**
Prepares you to pass the current CISSP® certification exam. An accelerated course that assumes the student has an understanding of networks and operating systems, and focuses on the eight domains of knowledge as determined by (ISC)². [www.sans.org/MGT414](www.sans.org/MGT414)

**MGT433: SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program**
Learn key concepts and skills to establish a mature security awareness program that turns your biggest risk into your greatest asset. [www.sans.org/MGT433](www.sans.org/MGT433)

**MGT512: Security Leadership Essentials for Managers**
Designed to empower managers who want to learn quickly on InfoSec issues and terminology. Learn security and how to manage security. [www.sans.org/MGT512](www.sans.org/MGT512)

**MGT514: IT Security Strategic Planning, Policy, and Leadership**
Be a security business leader who builds and executes strategic plans that resonate with other business executives, creates effective information security policy, and develops management skills to better lead, inspire, and motivate teams. [www.sans.org/MGT514](www.sans.org/MGT514)

## Audit Curriculum

**AUD507: Auditing and Monitoring Networks, Perimeters, and Systems**
Provides a risk-driven method to design an enterprise security-validation program. Covers a variety of high-level audit issues and general audit best practices. Learn to dive deep into the technical how-to for determining the key controls used to provide a level of assurance to an organization. [www.sans.org/AUD507](www.sans.org/AUD507)

## Legal Curriculum

**LEG523: Law of Data Security and Investigations**
Teaches the law of business, contracts, fraud, crime, IT security, IT liability and IT policy – all with a focus on electronically stored and transmitted records. Investigators will learn how to prepare credible, defensible reports, whether for cyber crimes, forensics, incident response, human resources or other investigations. [www.sans.org/LEG523](www.sans.org/LEG523)

## DevSecOps Curriculum

**DEV522: Defending Web Applications Security Essentials**
Learn how to defend web applications – traditional network defenses like firewalls fail to secure web applications. The quantity and importance of data entrusted to web applications is growing and defenders need to learn how to secure that data. [www.sans.org/DEV522](www.sans.org/DEV522)

**SEC534: Secure DevOps: A Practical Introduction**
Explains the fundamentals of DevOps, and how teams can build and deliver secure software. Learn how to leverage the principles, practices and tools to improve the reliability, integrity and security of systems. [www.sans.org/SEC534](www.sans.org/SEC534)

**SEC540: Cloud Security and DevOps Automation**
Master the tools needed to build and deliver secure software using DevOps and cloud services, specifically Amazon Web Services (AWS). Explore how the principles, practices, and tools of DevOps and AWS can improve the reliability, integrity, and security of applications. [www.sans.org/SEC540](www.sans.org/SEC540)

**DEV541: Secure Coding in Java/JEE: Developing Defensible Applications**
Learn how to build secure Java applications and gain skills to keep a website from getting hacked, counter a wide range of application attacks, prevent critical security vulnerabilities, and understand attackers. [www.sans.org/DEV541](www.sans.org/DEV541)

**DEV544: Secure Coding in .NET: Developing Defensible Applications**
Leverage built-in and custom defensive technologies to integrate security into applications. Examine actual code, work with real tools, build applications, and gain confidence in the resources you need to add to the security of .NET applications. [www.sans.org/DEV544](www.sans.org/DEV544)

## Industrial Control Systems Curriculum

**ICS410: ICS/SCADA Security Essentials**
Designed to train the workforce involved in supporting and defending industrial control systems how to keep the operational environment safe, secure, and resilient against current and emerging threats. [www.sans.org/ICS410](www.sans.org/ICS410)

**ICS515: ICS Active Defense and Incident Response**
Deconstruct ICS cyber attacks, leverage an active defense to identify and counter threats in your ICS, and maintain the safety and reliability of operations. Understand your networked ICS environment, monitor it for threats, perform incident response against identified threats, and learn from interactions to enhance network security. [www.sans.org/ICS515](www.sans.org/ICS515)
<table>
<thead>
<tr>
<th>Cyber Defense</th>
<th></th>
<th></th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC301: Introduction to Cyber Security</td>
<td>•</td>
<td>•</td>
<td>GISP</td>
</tr>
<tr>
<td>SEC401: Security Essentials Bootcamp Style</td>
<td>•</td>
<td>•</td>
<td>GSF</td>
</tr>
<tr>
<td>SEC440: Critical Security Controls: Planning, Implementing, and Auditing</td>
<td>•</td>
<td>•</td>
<td>GSEC</td>
</tr>
<tr>
<td>SEC455: SIEM Design &amp; Implementation</td>
<td>•</td>
<td>•</td>
<td>$2,640</td>
</tr>
<tr>
<td>SEC467: Open-Source Intelligence (OSINT) Gathering and Analysis</td>
<td>•</td>
<td>•</td>
<td>$6,610</td>
</tr>
<tr>
<td>SEC501: Advanced Security Essentials – Enterprise Defender</td>
<td>•</td>
<td>•</td>
<td>GCCED</td>
</tr>
<tr>
<td>SEC503: Intrusion Detection In-Depth</td>
<td>•</td>
<td>•</td>
<td>GCIA</td>
</tr>
<tr>
<td>SEC505: Securing Windows and PowerShell Automation</td>
<td>•</td>
<td>•</td>
<td>GCWN</td>
</tr>
<tr>
<td>SEC506: Securing Linux/Unix</td>
<td>•</td>
<td>•</td>
<td>GCUX</td>
</tr>
<tr>
<td>SEC511: Continuous Monitoring and Security Operations</td>
<td>•</td>
<td>•</td>
<td>GMON</td>
</tr>
<tr>
<td>SEC524: Cloud Security and Risk Fundamentals</td>
<td>•</td>
<td>•</td>
<td>$2,640</td>
</tr>
<tr>
<td>SEC530: Defensible Security Architecture and Engineering</td>
<td>•</td>
<td>•</td>
<td>GDSA</td>
</tr>
<tr>
<td>SEC545: Cloud Security Architecture and Operations</td>
<td>•</td>
<td>•</td>
<td>$5,730</td>
</tr>
<tr>
<td>SEC555: SIEM with Tactical Analytics</td>
<td>•</td>
<td>•</td>
<td>GCDA</td>
</tr>
<tr>
<td>SEC566: Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td>•</td>
<td>•</td>
<td>GCCC</td>
</tr>
<tr>
<td>SEC599: Defeating Advanced Adversaries – Purple Team Tactics &amp; Kill Chain Defenses</td>
<td>•</td>
<td>•</td>
<td>GDAT</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Penetration Testing</th>
<th></th>
<th></th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC460: Enterprise Threat and Vulnerability Assessment</td>
<td>•</td>
<td>•</td>
<td>$6,610</td>
</tr>
<tr>
<td>SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td>•</td>
<td>•</td>
<td>GCIH</td>
</tr>
<tr>
<td>SEC542: Web App Penetration Testing and Ethical Hacking</td>
<td>•</td>
<td>•</td>
<td>GWAPT</td>
</tr>
<tr>
<td>SEC560: Network Penetration Testing and Ethical Hacking</td>
<td>•</td>
<td>•</td>
<td>GPEN</td>
</tr>
<tr>
<td>SEC573: Automating Information Security with Python</td>
<td>•</td>
<td>•</td>
<td>GPYC</td>
</tr>
<tr>
<td>SEC575: Mobile Device Security and Ethical Hacking</td>
<td>•</td>
<td>•</td>
<td>GMOB</td>
</tr>
<tr>
<td>SEC617: Wireless Penetration Testing and Ethical Hacking</td>
<td>•</td>
<td>•</td>
<td>GAWN</td>
</tr>
<tr>
<td>SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques</td>
<td>•</td>
<td>•</td>
<td>$6,610</td>
</tr>
<tr>
<td>SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking</td>
<td>•</td>
<td>•</td>
<td>GXPN</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Incident Response &amp; Forensics</th>
<th></th>
<th></th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOR500: Windows Forensic Analysis</td>
<td>•</td>
<td>•</td>
<td>GCFE</td>
</tr>
<tr>
<td>FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics</td>
<td>•</td>
<td>•</td>
<td>GCFA</td>
</tr>
<tr>
<td>FOR518: Mac and iOS Forensic Analysis and Incident Response</td>
<td>•</td>
<td>•</td>
<td>$6,610</td>
</tr>
<tr>
<td>FOR526: Advanced Memory Forensics &amp; Threat Detection</td>
<td>•</td>
<td>•</td>
<td>$6,610</td>
</tr>
<tr>
<td>FOR527: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response</td>
<td>•</td>
<td>•</td>
<td>GNFA</td>
</tr>
<tr>
<td>FOR578: Cyber Threat Intelligence</td>
<td>•</td>
<td>•</td>
<td>GCTI</td>
</tr>
<tr>
<td>FOR585: Smartphone Forensic Analysis In-Depth</td>
<td>•</td>
<td>•</td>
<td>GASF</td>
</tr>
<tr>
<td>FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td>
<td>•</td>
<td>•</td>
<td>GREM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Management</th>
<th></th>
<th></th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGT414: SANS Training Program for CISSP® Certification</td>
<td>•</td>
<td>•</td>
<td>GISP</td>
</tr>
<tr>
<td>MGT433: Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program</td>
<td>•</td>
<td>•</td>
<td>$2,640</td>
</tr>
<tr>
<td>MGT512: Security Leadership Essentials for Managers</td>
<td>•</td>
<td>•</td>
<td>GSLC</td>
</tr>
<tr>
<td>MGT514: IT Security Strategic Planning, Policy, and Leadership</td>
<td>•</td>
<td>•</td>
<td>GSTRT</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DevSecOps</th>
<th></th>
<th></th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEV532: Defending Web Applications Security Essentials</td>
<td>•</td>
<td>•</td>
<td>GWEB</td>
</tr>
<tr>
<td>SEC534: Secure DevOps: A Practical Introduction</td>
<td>•</td>
<td>•</td>
<td>$2,640</td>
</tr>
<tr>
<td>SEC540: Cloud Security and DevOps Automation</td>
<td>•</td>
<td>•</td>
<td>$5,730</td>
</tr>
<tr>
<td>DEV541: Secure Coding in Java/JEE: Developing Defensible Applications</td>
<td>•</td>
<td>•</td>
<td>$5,180</td>
</tr>
<tr>
<td>DEV544: Secure Coding in .NET: Developing Defensible Applications</td>
<td>•</td>
<td>•</td>
<td>$5,180</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Audit</th>
<th></th>
<th></th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUD507: Auditing &amp; Monitoring Networks, Perimeters, and Systems</td>
<td>•</td>
<td>•</td>
<td>GSNA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Legal</th>
<th></th>
<th></th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEG523: Law of Data Security and Investigations</td>
<td>•</td>
<td>•</td>
<td>GLEG</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Industrial Control Systems</th>
<th></th>
<th></th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICS410: ICS/SCADA Security Essentials</td>
<td>•</td>
<td>•</td>
<td>GICSP</td>
</tr>
<tr>
<td>ICS515: ICS Active Defense and Incident Response</td>
<td>•</td>
<td>•</td>
<td>GRID</td>
</tr>
</tbody>
</table>
Create a **SANS Account** today to enjoy these free resources at [www.sans.org/account](http://www.sans.org/account)

### Newsletters

**NewsBites**
Twice-weekly, high-level executive summary of the most important news relevant to cybersecurity professionals.

**OUCH!**
The world’s leading monthly free security awareness newsletter designed for the common computer user.

### Webcasts

**Ask the Experts Webcasts**
SANS experts bring current and timely information on relevant topics in IT Security.

**Analyst Webcasts**
A follow-on to the SANS Analyst Program, Analyst Webcasts provide key information from our whitepapers and surveys.

### Other Free Resources

- InfoSec Reading Room
- Top 25 Software Errors
- 20 Critical Controls
- Security Policies
- Intrusion Detection FAQs
- Tip of the Day

### Course Demos

Test Drive more than 40 SANS courses and decide which is right for you. Our demos are delivered via the SANS OnDemand platform, and give you a close look at a course’s contents, pace, and features.

[www.sans.org/demo](http://www.sans.org/demo)

### Exclusive Special Offers

Choose a **tablet, laptop, or course discount** offer with select OnDemand and vLive courses.

For more details, visit: [www.sans.org/online](http://www.sans.org/online)
### Platform Features
- **Simulcast**
  - Taught live by the same faculty of information security educators.
  - Same classroom experience as live SANS training including books, media, and exercises.
  - Property in-learning platform available for a box or keg.
  - Live evening meetings in 5 or 6 weeks.
- **vLive**
  - Simultaneous access to three states: Multistate Security Symposium.
  - Integrate lessons in Real-time learning.
  - Subject Matter Expert support via Live Chat and Email.
  - Real-time access to instructors.

### OnDemand Features
- **SelfStudy**
  - Up to 35 questions available for training and exam preparation.
  - Available certifications in over 20 specializations.
  - Designed to deliver the benefits of live seminars across the country.
- **vLive**
  - Real-time interactions with peers and expert faculty.
  - Provides a dynamic learning environment.

### Cybersecurity

#### Job Roles | Skills | SANS Courses

**Use the Course Roadmap to Select a Career Path and to Create Your SANS Training Plan**

#### Packaging matters

**Write a formal request**

- All organizations are a bit different, but better thinking requires a better request.
  - Be sure to understand the context for the event.
  - Make sure the request is consistent with the organization’s training or performance goals.
  - Establish a timeline for the event.

**Clearly state the benefits**

- **Set the context**
  - Clearly state the context.
  - Include the benefits of the training.
  - Place the particular course you wish to take into the context of your role.
  - Write a formal request.

**Establish longer-term expectations**

- Information security is a broad and diverse field. Don’t make an absolute change in demeanor from the get-go. It’s not a one-time event. It’s an ongoing commitment.
  - **One week of training is just a beginning.**
  - **Two weeks of training is a start.**
  - **Three or more weeks is a substantial investment.**

**OnDemand and Budget for Training**

**Budget for Training**

- **Write a formal request.**
  - Consider offering trade-offs for the investment.
  - Take a GIAC Certification exam to prove the training worked.

**Secure a training budget**

- **Financial Impact**
  - Establish longer-term expectations.
  - Be specific.
  - Make sure the request is consistent with the organization’s training or performance goals.
  - Provide all the necessary information in one place.
  - All organizations are different, but because training requires a dynamic field is an annual, per-person expense, and not a once-and-done item.
  - Many professionals build annual training expense into their employment agreements even before joining a company.

**Cybersecurity**

**Job Roles | Skills | SANS Courses**

**Use the Course Roadmap to Select a Career Path and to Create Your SANS Training Plan**

#### Private Training

**Conflict of training programs (the same tools, the same methods, etc.) must be built for the same learning outcomes.**

**Private Training Bundles**

**OnDemand Bundles**

**SelfStudy**

**SANS Online Training**

SANS Online Training is ideal preparation for GIAC Certification Exams.

**35 questions**

35 questions are available for training and exam preparation. In order to earn the GIAC Certified Exam. Visit www.sans.org/onlinedata for more information.

**Contact us at:**

contact@sans.org | www.sans.org/online-training
Build a High-Performing Security Organization

SANS recommends these strategies for building an information security team, based on research and long-term observations globally:

1. Use Practical Organizing Principles
   - Identify risk in tangible terms by estimating losses and estimating risks, prioritizing, and assigning resources, probably with some quantifying, to respond to identified risks.
2. Implement Known Security Controls
   - Prioritize your efforts within your group framework using the Center for Internet Security's 20 Critical Security Controls. The controls are a good template for creating your cybersecurity framework.
3. Evaluate and Empower Your People
   - Expand the number and type of professionals required for your organization's particular needs and to face current threats (use the chart below as a guideline). Engage in a persistent campaign to develop appropriate hands-on, essential security skills and techniques.

The detection of what is happening in your environment requires an increasingly active defense, as threats become more sophisticated. While you must know your underlying infrastructure well, you don't need hands-on skills to operate it. What you need is that finding vulnerabilities requires a different way of thinking, and different tools, in order to perform the type of analysis and assessment required to manage your environment.

With an increasing number of talented technologists, organizations require effective leaders to manage their teams and processes. Those managers will not necessarily have the hands-on skills required to work in the high-level infrastructure and determine where those skills are needed. They need to determine the number and type of professionals required to meet your organization's particular needs and to face current threats (use the chart below as a guideline). Engage in a persistent campaign to develop appropriate hands-on, essential security skills and techniques.

Nearly all of your complex information security tasks and frameworks can be contained within four or five simple categories. Use practical organizing principles and known security controls to prioritize your efforts and evaluate people. Implement known security controls in your organization.

With a few exceptions, you are responsible for managing security teams or implementing and auditing the critical security controls—In-depth, Intrusion Detection, Monitoring Over Time, In-Depth Coverage, and Defensible Security Architecture. Whether you choose to maintain a formal education in a broad range of technologies, you will need to determine where those skills are needed. You need to determine the number and type of professionals required to meet your organization's particular needs and to face current threats (use the chart below as a guideline). Engage in a persistent campaign to develop appropriate hands-on, essential security skills and techniques.

People & Skills = Size of Organization, Value at Risk

1. Core Techniques
   - Core Techniques are the foundation for cybersecurity professionals to learn and practice. They include hands-on, essential security skills and techniques that are critical to the cybersecurity professional's success.

2. Security Management & Technical Architectures
   - Security Management can be divided into three main categories: Leadership, Management, and Technical Architectures. Leadership is the most important aspect of cyber security management, as it sets the tone for the organization and determines how to prioritize efforts.

3. Testing & Research
   - Testing & Research is a critical component of cybersecurity, as it helps organizations identify and mitigate threats.

4. Professional Skills
   - Professional Skills include hands-on, essential security skills and techniques that are critical to the cybersecurity professional's success.

5. Training Roadmap
   - Training Roadmap is a comprehensive guide to help organizations determine which training is needed for their teams. The roadmap includes a range of courses and certifications, from basic to advanced, to help organizations develop a robust cybersecurity program.

6. Development & Specialized Skills
   - Development & Specialized Skills are advanced skills and techniques that are necessary for cybersecurity professionals who are responsible for developing and implementing complex systems and applications.

7. Specialized Investigative Skills
   - Specialized Investigative Skills are advanced skills and techniques that are necessary for cybersecurity professionals who are responsible for investigating complex cyber incidents.

8. Other Advanced Defense Courses
   - Other Advanced Defense Courses are advanced skills and techniques that are necessary for cybersecurity professionals who are responsible for defending against advanced threats.

9. Language-Specific Courses
   - Language-Specific Courses are advanced skills and techniques that are necessary for cybersecurity professionals who are responsible for defending against threats in specific languages.

To learn more about additional SANS courses, visit: www.sans.org.

For assistance in navigating the roadmap, or in planning your team’s training strategy, contact SANS at training@sans.org or 610-688-8333.